Remarks

Claims 1-20 are pending in the application. Claims 1-20 were rejected. Claim 1 is the independent claim. Reconsideration of the application in view of the following remarks is respectfully requested.

The examiner rejected claim 1 under 35 USC §102(e) as being anticipated by Fieres et al.

Amended claim 1 recites a process of checking the authorization and authenticity of an application for use by a user on a device within a domain. The process includes authenticating an application authentication file against a domain administrator's public membership key, checking the application authentication file for one or more application identification and authorization objects, and hashing an application executable. The application hash result is compared to an authentication hash contained in the application authentication file. Services to the application are denied if the application hash and the authentication hash do not match. The application identification and authorization objects are decoded if the application hash and the authentication hash match. The decoded application identification and authorization objects are compared to domain identification and authorization objects associated with the domain. Services are provided to the application if the result of the domain comparison is favorable, and services are denied to the application if the result of the domain comparison is not favorable.

Thus, claim 1 describes a process by which an application is checked for identity and authentication. The domain specifies which applications are valid for use within the

domain, and comparisons are made to determine that the application is allowed for use in the domain and that the application has not been changed since authorization. Claims 2-20 recite further checks, for example as to whether the user is identified and authenticated for use of the application, and authenticated for use of the application on the particular device.

In contrast, Fieres et al. discloses host system elements for an international cryptography framework. The application support elements include application authentication, by which a hash sum of the application code image, the application ID, and classes of service assigned to the application are authenticated by means of a digital signature. The class of service concept includes a trusted description of the application resource map and attributes that express the application's capabilities. The classes of service are mapped and analyzed when an application is called, so that suitable applications having the least capable classes of service are selected for a task. See column 8, line 47 through column 9, line 3; column 10, lines 45-59; and column 12, lines 11-20.

The examiner stated that Fieres et al. teach authenticating the information using a digital signature, where it is inherent that a key is necessary and present to validate the signature, in the passage at col. 8, lines 49-55. This passage describes that cryptography framework applications can be certified, wherein the certificate includes identifying attributes of the application, including the application ID, a hash sum of the application code image, and the classes of service assigned to the application. The information in the

certificate is authenticated by a digital signature. The certificate is used for identification and access authorization of the application.

The examiner stated that Fieres et al. teach hashing a sum of the application code image, in the passage at col. 8, line 51. That passage describes that the certificate includes a hash sum of the application code image. It is not clear from the disclosure that the code image is an application executable.

The examiner stated that Fieres et al. teach a certificate contains identifying attributes of the application which are used to accurately identify an application, in the passage at col. 8, lines 49-55. This passage describes that cryptography framework applications can be certified, wherein the certificate includes identifying attributes of the application, including the application ID, a hash sum of the application code image, and the classes of service assigned to the application. The information in the certificate is authenticated by a digital signature. The certificate is used for identification and access authorization of the application.

The examiner stated that Fieres et al. teach that a signature validation process can be applied to the applet to verify that the applet has been signed by a trusted entity, in the passage at col. 10, lines 32-34. This is what is described in the cited passage, but it is not clear how this disclosure applies to the features of claim 1.

The examiner stated that Fieres et al. teach where the applet is allowed to run after integrity checks are confirmed, in the passage at col. 10, lines 34 and 35. Again, this is what is described in the cited passage, but it is not clear how this disclosure applies to the

features of claim 1. The vague disclosure of "some further integrity checks" does not read on the specific features recited in claim 1.

The examiner stated that Fieres et al. teach the architecture provides the concepts of a class of service where COS identifiers label the resource, in the passage at col. 10, lines 45-49. Again, this is what is described in the cited passage, but it is not clear how this disclosure applies to the features of claim 1. Claim 1 does not recite labeling of an application resource.

The examiner stated that Fieres et al. teach acquiring access to resources according to the application assigned capabilities and executing application methods in a secure location, in the passage at col. 10, lines 51-59. That passage actually describes that the resource map class of service cannot be manipulated to acquire access to resources beyond the application assigned capabilities. This might imply that the resource map COS is a necessary component to acquire access to resources, but it is not clear how this disclosure applies to the features of claim 1. Further, the passage does describe that the cryptographic unit can execute application methods in a secured location, but again it is not clear how this disclosure applies to the features of claim 1. Claim 1 recites a process of checking the authorization and authenticity of an application, and does not recite executing the application in a secured location.

The examiner stated that Fieres et al. teach they [the descriptive part of a COS identifier] are signed by the ICF domain authority and the COS identifiers are evaluated before access to the method is granted, in the passage at col. 11, lines 13-16. This passage discloses that a class of service consists of a COS identifier, for example, a

number, and a descriptive part that contains the identifier of the associated application method and constraints that must be evaluated before access to the application method will be granted. The descriptive part is signed by an authority (not disclosed as the ICF domain authority) to assure authenticity and integrity. Thus, the identifier of the application is signed for authenticity, but it is not disclosed that it is signed by an ICF domain authority or any other domain authority. Fieres et al. disclose that the application can be signed by the application provider (see col. 10, lines 32-34), but do not disclose here that it is signed by a domain authority.

The examiner stated that Fieres et al. teach requested attributes are compared to a set of privilege attributes where if the result is positive the caller is allowed to go ahead, and it is inherent that if the result is negative then services are denied, in the passage at col. 12, lines 23-26. This passage (the entire passage is found at col. 12, lines 11-27) describes an authorization engine that can implement a COS mapping scheme by which a least capable COS is selected from among a list of authorized applications. The caller, which is seeking to select an application for a desired operation, passes its request attributes, which are compared to a set of matching privilege attributes. If a positive match is found, that is, if an application that can provide the desired operation is found, that application is selected. If more than one application can provide the desired operation, the least capable application is selected. If a match is not found, the call goes unsatisfied. Thus, this is a process by which applications, which have already been authorized for use with the CU, are selected based on functionality for specific operations required by a caller. This is not an authorization and authentication function, that is,

these applications have already been authorized and authenticated, and have been mapped according to functionality attributes of the application. The caller is looking for applications that satisfy its functional requirements. If one is found, it is selected. If one is not found, it means that the functionality cannot be satisfied; it does not mean that an application is rejected because it has not been authenticated. The features described in this passage are unrelated to those recited in claim 1.

The examiner stated that Fieres et al. teach checking the application authentication file for one or more application identification and authorization objects, in the passage at col. 6, lines 26-38. This passage describes that the ADA receives COS elements granted by the SDA and issues application certificates to the applications belonging to its domains. The certificates include the application ID and the COS. The certificate is presented to the CU to get a COS level. The appropriate level is granted by the CU based on the contents of the certificate. This passage does not define what is included in the COS elements, or what a COS level is. Later, at col. 11, lines 13-18, a COS identifier and a descriptive part are disclosed, which must be evaluated before a method (application) is granted to a caller. Thus, the application is identified, and its attributes are evaluated before the application is released to a caller. See col. 12, lines 11-27, where it is clearly disclosed that the attributes are functional attributes, not authentication attributes. Applications belonging to a domain are available to callers, which seek applications having particular functional attributes. Thus, an application authentication file is not checked for identification and authorization objects prior to allowing use of the application on a device, as recited in claim 1. Rather, callers seeking

applications having certain functional attributes determine if an application is suitable by examining COS elements of the application.

In view of the above, it is submitted that Fieres et al. disclose an international cryptography framework by which host system elements are made available based on functionality and compatibility with various disparate domains, prior to gaining access to cryptographic services provided by the system. See col. 2, lines 35-44. Each domain supplies applications, which are categorized by class of service by their respective domains, and which are made available to callers from other domains, which callers select applications, if available, according to functional attributes included in the COS elements. Fieres et al. do not disclose or suggest checking the identity and authentication of an application for valid use within a domain. Rather, Fieres et al. check attributes of an application to select a suitable and least-capable application for use in response to a call, and check the selected application for modification. Fieres et al. also do not disclose checking I&A attributes of a user and/or a device before allowing use of an application within the domain by the user on the user's device.

Thus, the cited reference discloses an invention that is fundamentally different than that recited in claim 1. For example, Fieres et al. do not disclose checking the application authentication file for one or more application identification and authorization objects. Further, Fieres et al. do not disclose, and the examiner did not assert that the reference discloses, comparing an application hash result to an authentication hash contained in the application authentication file; denying services to the application if the application hash and the

authentication hash do not match; decoding the one or more application identification and authorization objects if the application hash and the authentication hash match; comparing the decoded one or more application identification and authorization objects to domain identification and authorization objects associated with the domain; providing services to the application if the result of the domain comparison is favorable; and denying services to the application if the result of the domain comparison is not favorable, all as recited in claim 1.

For at least the reasons noted above, Fieres et al. do not anticipate the invention as recited in claim 1. The rejection of claim 1, therefore, should be withdrawn.

The examiner rejected claim 2 as being unpatentable over Fieres et al.; claims 3-6, 9, 10, and 13-20 as being unpatentable over Fieres et al., in view of Thomlinson et al.; and claims 7, 8, 11, and 12 as being unpatentable over Fieres et al., in view of Thomlinson et al. and Subbiah et al. The deficiencies of the Fieres et al. reference with respect to anticipating the invention recited in claim 1 are noted above. Neither Thomlinson et al. nor Subbiah et al. overcomes the deficiencies of the Fieres et al. disclosure. It is therefore submitted that no combination of the teachings of these references could render obvious the invention as recited in claims 2-20, which depend from claim 1. The rejections of claims 2-20, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

Respectfully submitted,

February 14, 2006
Date

Thomas M. Champagne
Registration No. 36,478
IP STRATEGIES
12 ½ Wall Street
Suite I
Asheville, North Carolina 28801
828.253.8600
828.253.8620 fax

TMC:hlp